09/481847

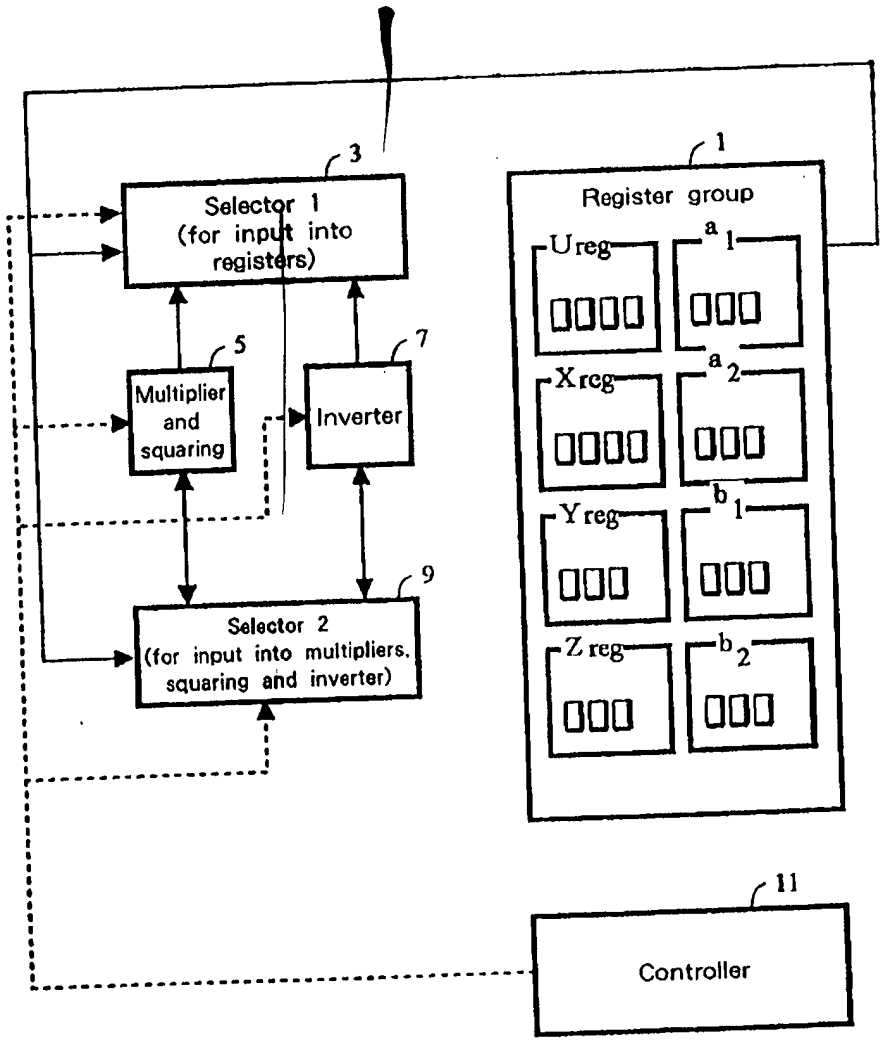


Fig. 1

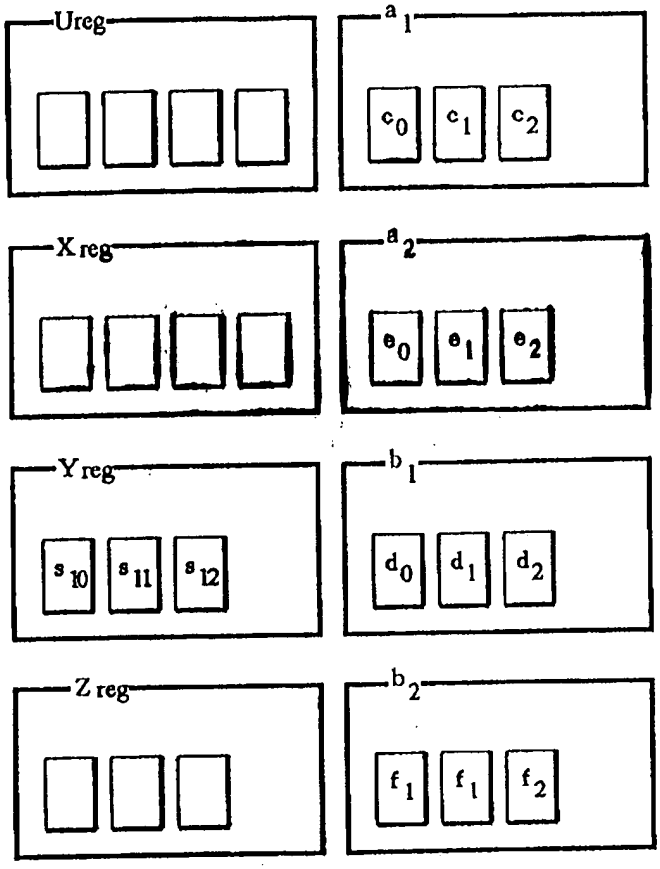
Ureg
a 1
c0 c1 c2
X reg
a 2
e0 e1 e2
Y reg
b 1
s10 s11 s12
d0 d1 d2
Z reg
b 2
f1 f1 f2

Fig. 2

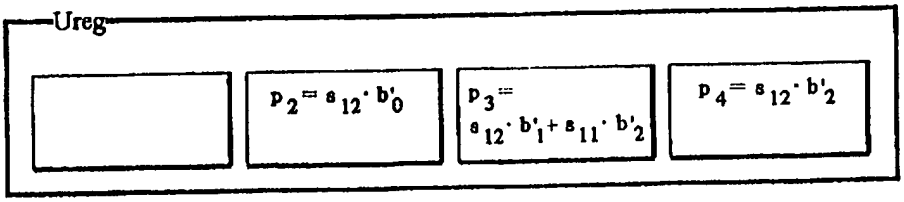
Ureg
p2 = s12 · b'0
p3 = s12 · b'1 + s11 · b'2
p4 = s12 · b'2

Fig. 3

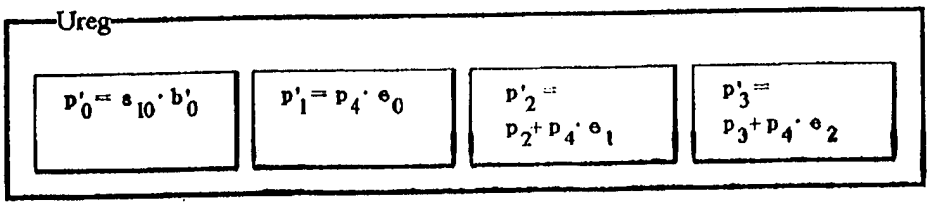


Fig. 4

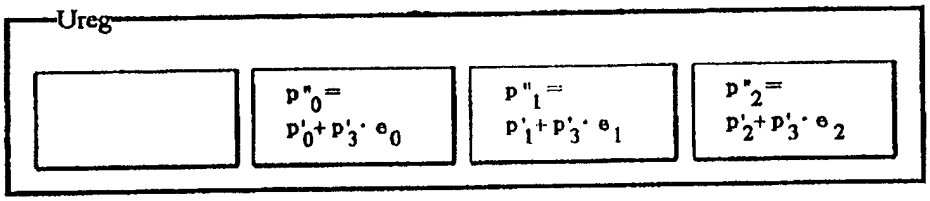


Fig. 5

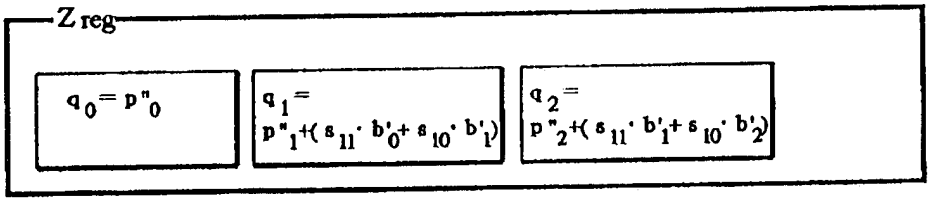


Fig. 6

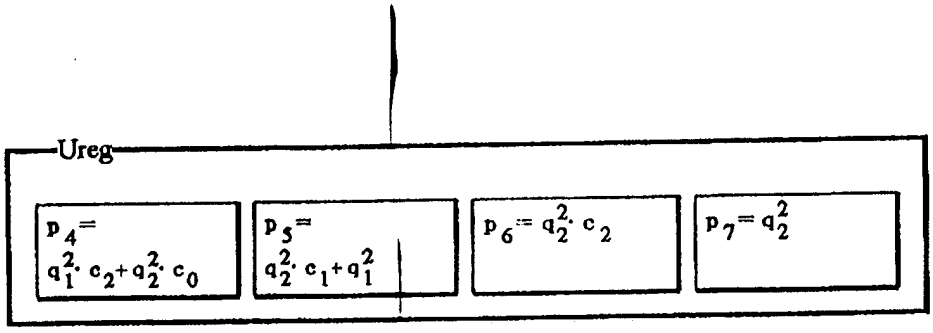


Fig. 7

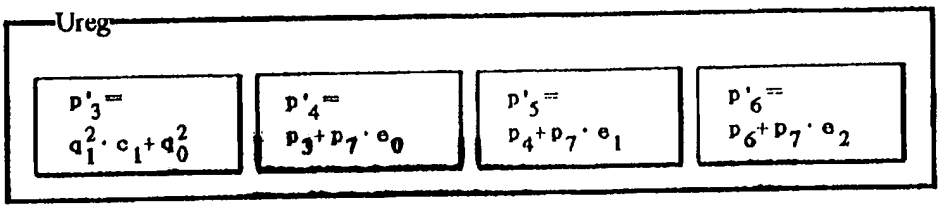


Fig. 8

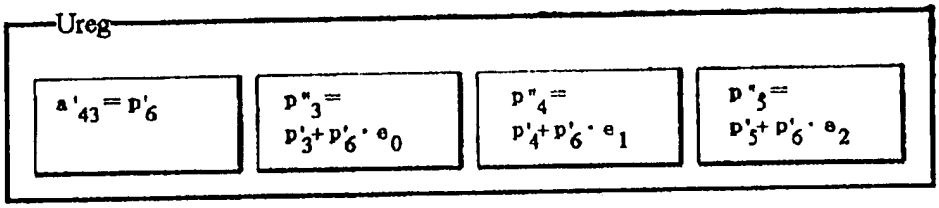


Fig. 9

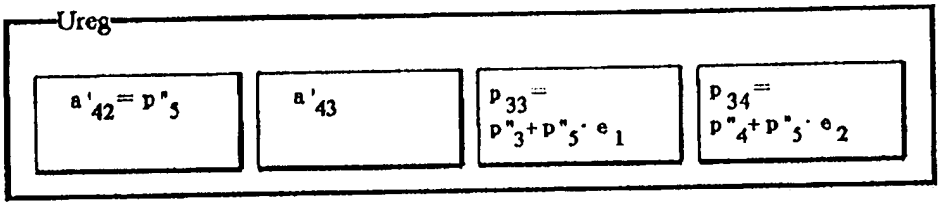


Fig. 10

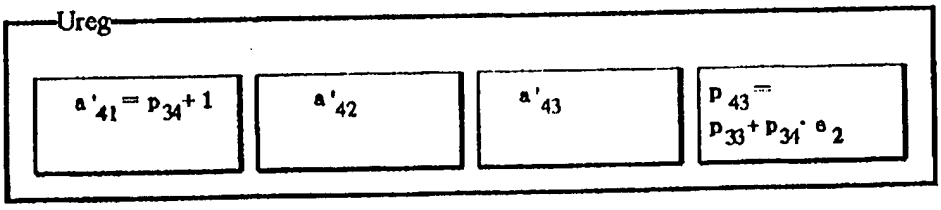


Fig. 11

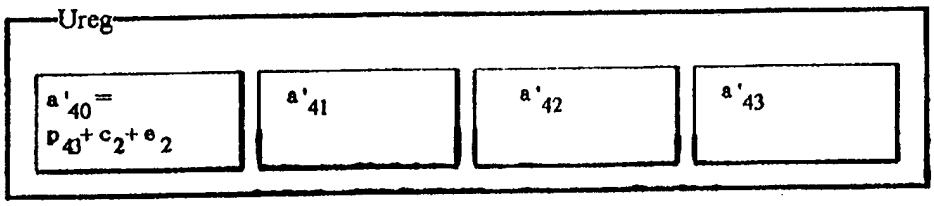


Fig. 12

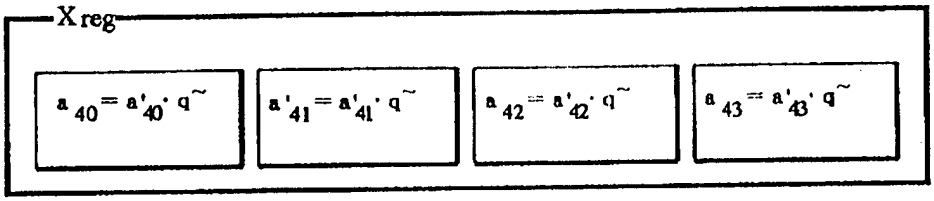


Fig. 13

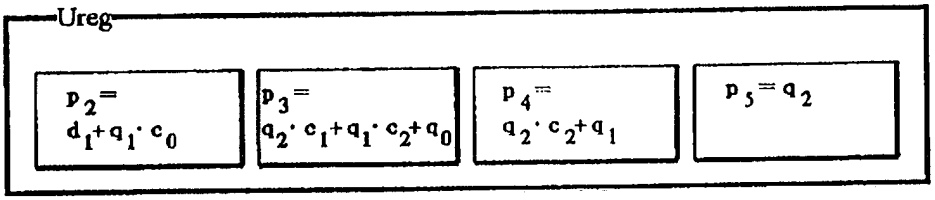


Fig. 14

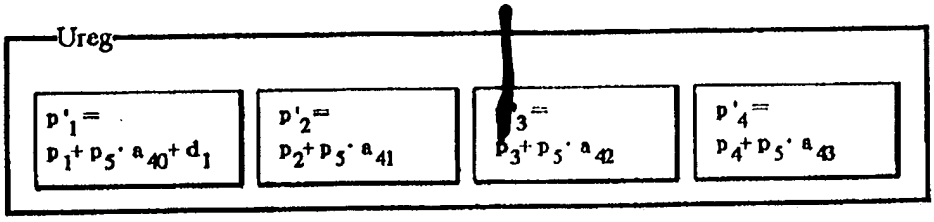


Fig. 15

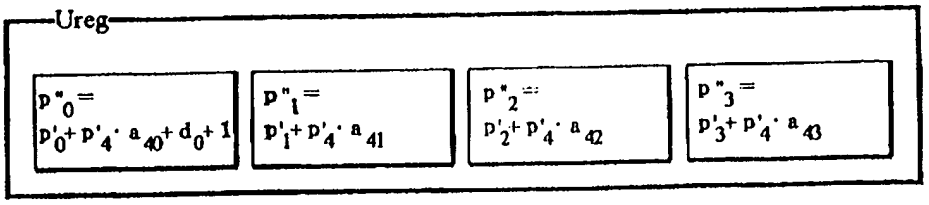


Fig. 16

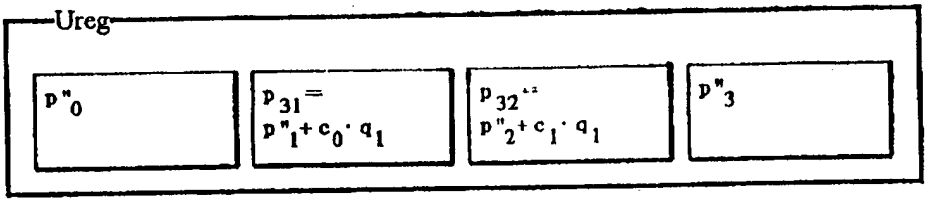


Fig. 17

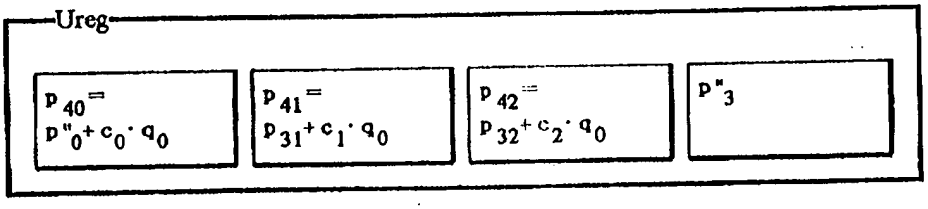


Fig. 18

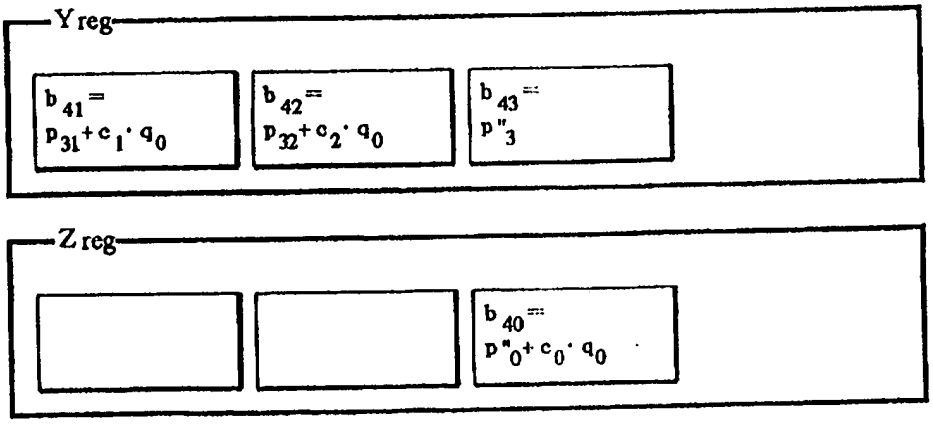


Fig. 19

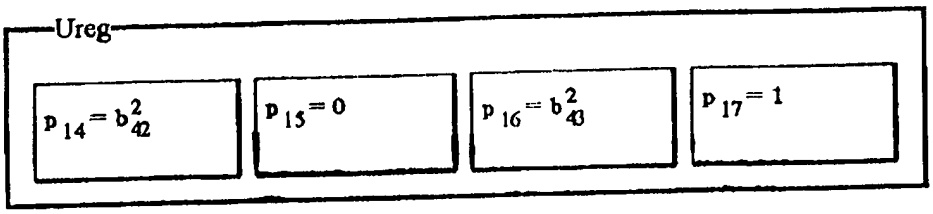


Fig. 20

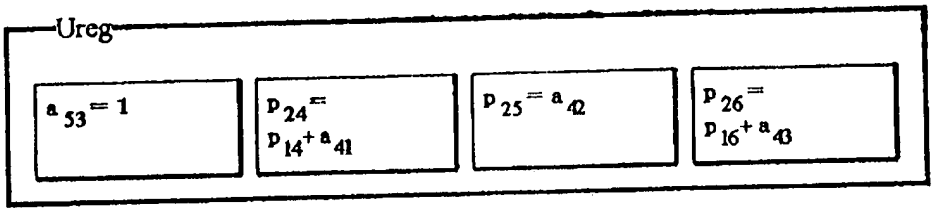


Fig. 21

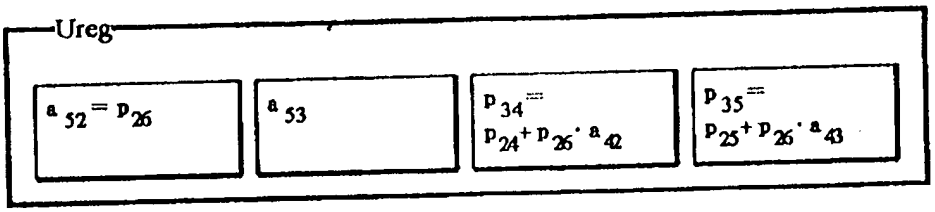


Fig. 22

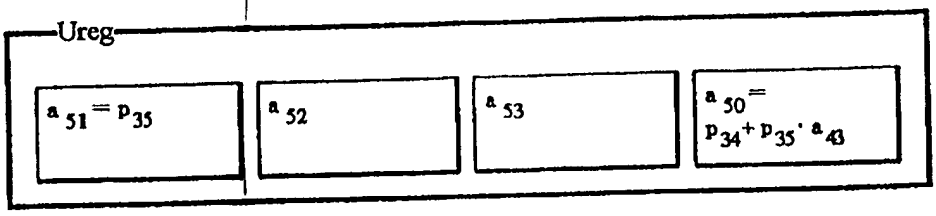


Fig. 23

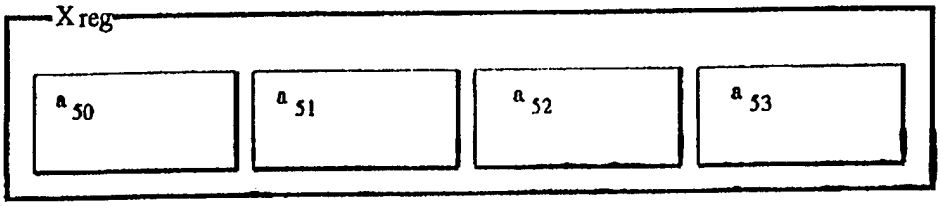


Fig. 24

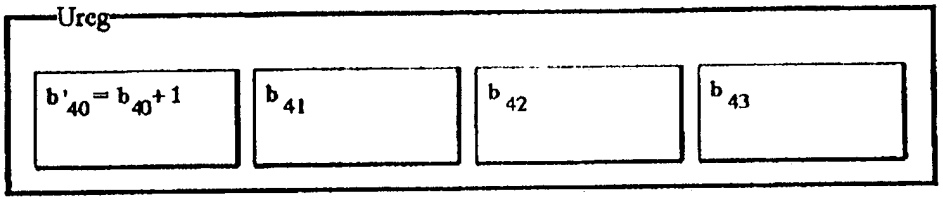


Fig. 25

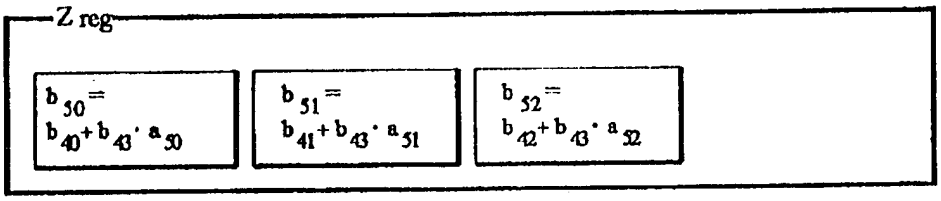


Fig. 26

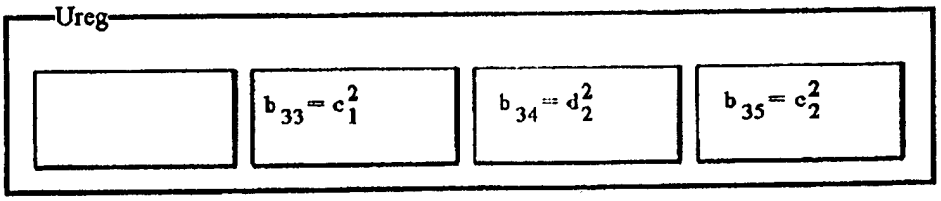


Fig. 27

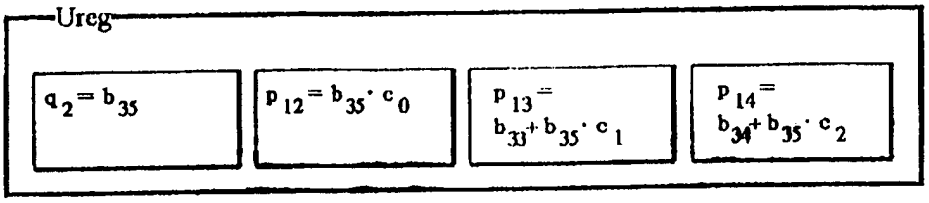


Fig. 28

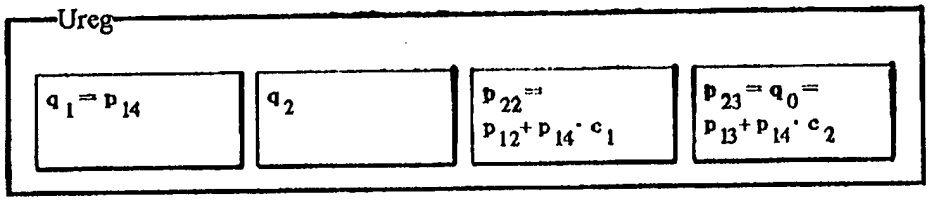


Fig. 29

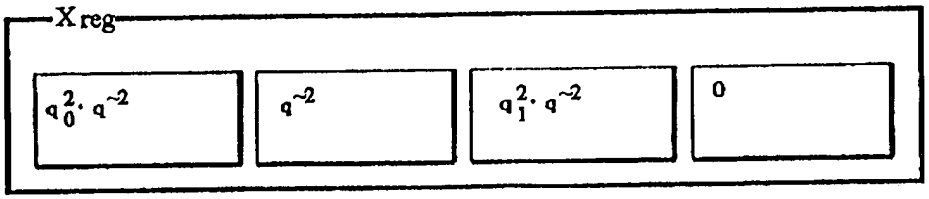


Fig. 30

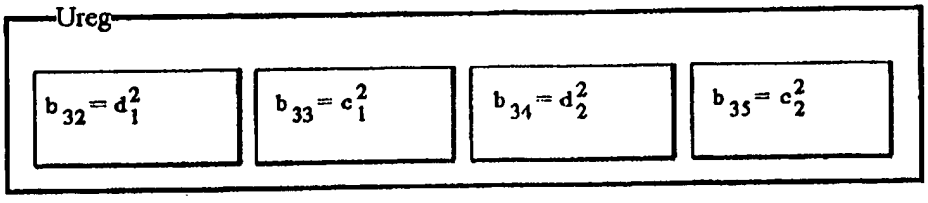


Fig. 31

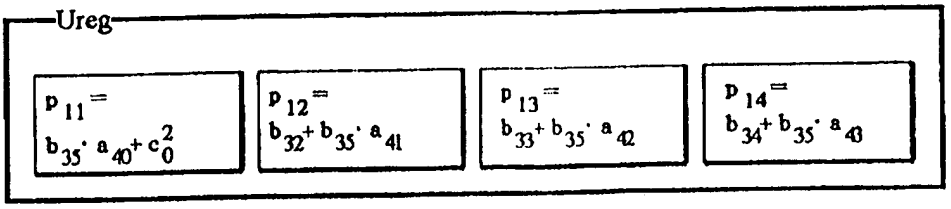


Fig. 32

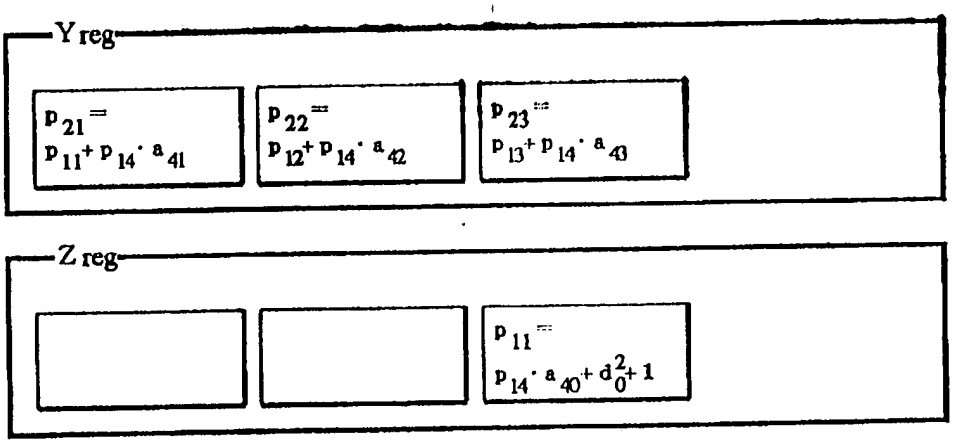


Fig. 33

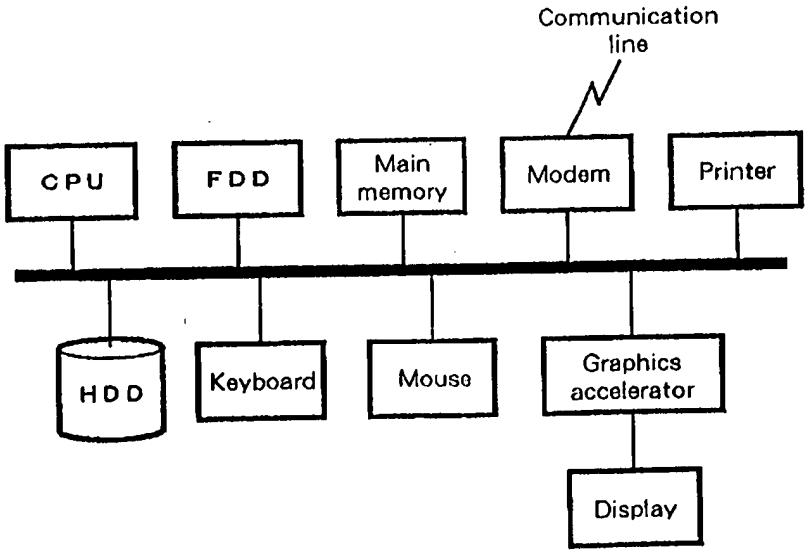


Fig. 35

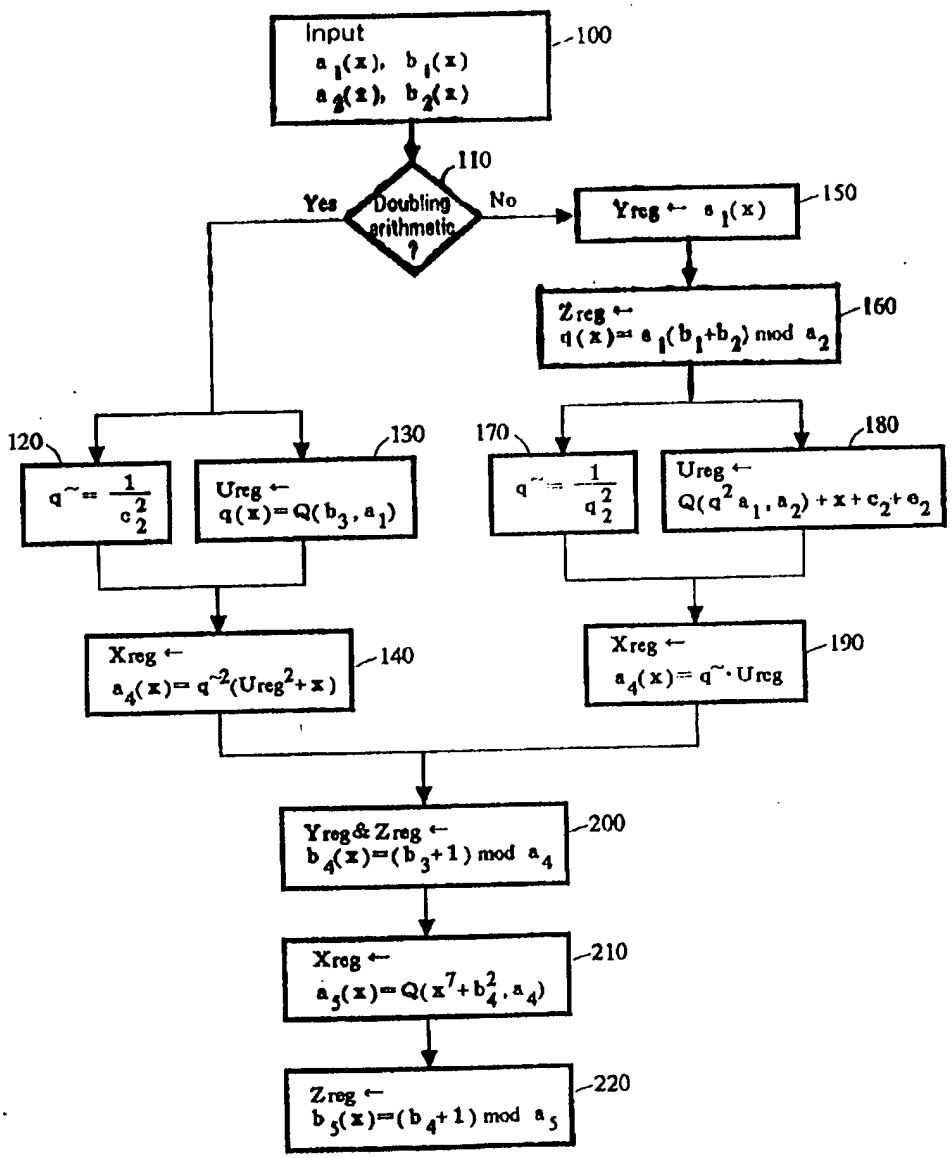
Input
$a_1(x)$, $b_1(x)$
$a_2(x)$, $b_2(x)$
100
110
Doubling arithmetic ?
Yes
No
Yreg ← $a_1(x)$
150
Zreg ←
$q(x) = a_1(b_1+b_2) \bmod a_2$
160
120
$q^{\sim} = \frac{1}{c_2^2}$
130
Ureg ←
$q(x) = Q(b_3, a_1)$
170
$q^{\sim} = \frac{1}{q_2^2}$
180
Ureg ←
$Q(q^2 a_1, a_2) + x + c_2 + e_2$
Xreg ←
$a_4(x) = q^{-2}(Ureg^2 + x)$
140
Xreg ←
$a_4(x) = q^{\sim} \cdot Ureg$
190
Yreg & Zreg ←
$b_4(x) = (b_3+1) \bmod a_4$
200
Xreg ←
$a_5(x) = Q(x^7 + b_4^2, a_4)$
210
Zreg ←
$b_5(x) = (b_4+1) \bmod a_5$
220

Fig. 34

[Expression 1]

$$D = \sum_{P_i \in C} m_i P_i$$

[Expression 2]

$$D_1 = \sum_{P_i \in C} m_i P_i$$

[Expression 3]

$$D_2 = \sum_{P_i \in C} n_i P_i$$

[Expression 4]

$$D_1 + D_2 = \sum_{P_i \in C} (m_i + n_i) P_i$$

[Expression 5]

$$div(h) = \sum_{P_i \in C} ord_{P_i}(h) P_i = \sum m_i P_i - \sum n_i Q_i$$

[Expression 6]

$$D_1 = \sum_{P_i \in C} m_i P_i - \left( \sum_{P_i \in C} m_i \right) P_\infty$$

[Expression 7]

$$\sum_{P_i \in C} m_i \leqq g$$

| Calculation | Computation complexity | Call frequency | Time |
|---|---|---|---|
| GCD | 3I+23m | 3I+9M | 3t(I)+9t(M) |
| q(x) | 15m | 4M | 4t(M) |
| $a_4(x)$ | I+20m | I+6M | t(I)+t(M) |
| $b_4(x)$ | 17m | 5M | 5t(M) |
| $a_5(x), b_5(x)$ | 6m | 3M | 3t(M) |
| Total | 4I+81m | 4I+27M | 4t(I)+22t(M) |

Table 1

| Calculation | Computation complexity | Call frequency | Time |
|---|---|---|---|
| q(x) | 3m | 2M | 0 |
| $a_4(x)$ | I+2m | I+M | t(I)+t(M) |
| $b_4(x)$ | 8m | 2M | 2t(M) |
| $a_5(x), b_5(x)$ | 6m | 3M | 3t(M) |
| Total | I+19m | I+8M | t(I)+6t(M) |

Table 2

| | Addition | | Doubling arithmetic | |
|---|---|---|---|---|
| | Multiplication | Multiplicative inverse computation | Multiplication | Multiplicative inverse computation |
| g=0 | 3 | 1 | 3 | 1 |
| g=3 | 401 | 0 | 265 | 0 |
| g=11 | 17477 | 0 | 10437 | 0 |

Table 3

| Operating frequency | Clock required for multiplying once | | |
|---|---|---|---|
| | Case A t (M) = 59 clock | Case B t (M) = 8 clock | Case C t (M) = 1 clock |
| 20MHz | 19.35ms | 2.624ms | 0.328ms |
| 40MHz | 9.68ms | 1.312ms | 0.164ms |
| 80MHz | 4.84ms | 0.656ms | 0.082ms |

Table 4

| Block in Fig. 1 | Size (cells) | |
|---|---|---|
| Multiplier | 34265 cells | 7 multipliers |
| Squaring | 1344 cells | 3 squaring operators |
| Inverter | 27414 cells | |
| Register group | 18408 cells | |
| Controller | 9749 cells | 26 59 – bit registers (including 12 coefficients) |
| Selector 1 | 37140 cells | |
| Selector 2 | 17402 cells | |
| Total | 145722 cells | |

Table 5